AMENDMENTS TO THE DRAWINGS:

A replacement drawing sheet of better quality (e.g., clear white background) than original Figure 1 is attached as an Appendix hereto in response to the drawing objection in the 5/18/2006 Office Action. No new matter is added.

Attachments: Replacement Drawing Sheet

Annotated Drawing Sheet Showing Changes

REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

As requested, a better quality drawing for Figure 1 is provided. Consequently, withdrawal of the objection to the drawings is respectfully requested.

Headings have been added to place the specification in a more traditional U.S. format. A grammatical error in the specification has been corrected.

Claims 1-12 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter. Applicant traverses this rejection and respectfully submits that the limitations in step/means c) of independent claims 1 and 7 do in fact constitute a practical application, not just an abstract idea. As stated in the office action, step/means c) in original claims 1 and 7 resulted in a signal indicating a file as known or unknown. Amended claims 1 and 7 further recite the indication as being malware, not malware or of unknown status.

The office action alleges that the claims relate to non-statutory subject matter because they do not "provide a tangible result as the results are not stored or displayed to the user." 6/18/2006 Office Action, page 7. However, Applicant respectfully submits that a signal is in fact a tangible result which has practical application. A signal is a technical entity that has a real existence inside a computer system. This signal has a physical presence in that it is represented by the internal physical state of components of the computer system. Thus, the requirement for signaling produces a tangible result in a similar manner as does, for example, a requirement for storing a result in memory.

Furthermore, a signal has a practical application because it provides real world value and provides an immediate benefit. This is because the signal allows the system (or user) to decide on how the file is subsequently handled. This is very much a real world benefit. By way of example without limitation, in the system of the described embodiment, the outputs 107 to 109 which provide support for the claimed signaling of

step/means c) are used to select the subsequent processing of the file to which they relate, as described on page 3, line 31 to page 4, line 5.

For at least these reasons, reconsideration and withdrawal of the Section 101 rejection of the pending claims is respectfully requested.

Claims 1-5 and 7-11 were rejected under 35 U.S.C. Section 102(e) as allegedly being "anticipated" by Roberts (U.S. Patent Application Publication No. 2004/088570). Claims 6 and 12 were rejected under 35 U.S.C. Section 103(a) as allegedly being "obvious" over Roberts in view of Wu et al. (U.S. Patent No. 5,617,533). While not acquiescing in these rejections, claims 1, 2, 5-8, 11 and 12 have been amended and the discussion below makes reference to the amended claims.

Throughout the claims, the references to a "virus" have been changed to "malware" in accordance with the description at page 1, lines 9-11.

Independent claim 1 has been amended to incorporate features of claims 3 and 4 and independent claim 7 has been amended to incorporate features of claims 9 and 10. Each of claims 1 and 7 now further specifies the manner in which the file being processed can be determined to be an instance of a known executable program. In particular, the step/means a) have been amended to further specify that the criteria stored in the database include "at least one characteristic signature associated with each said instance" and the step/means b) have been amended to specify determining whether the file is an instance of a known program by checking the contents of the file for the presence of the at least one characteristic signature.

Also, the step/means b) explicitly recites checking whether the file is an unchanged version of a known program.

Independent claims 1 and 7 have been further amended to further clarify the operation of step/means c) to specify the three operations for signaling the file as being: likely to be not malware; likely to be malware; or of unknown status. By way of example without limitation, support for such signaling can be found by referring to the three

outputs 107, 108 and 109 in the non-limiting, illustrative embodiment described in the subject patent application.

Claims 2 and 8 have been amended to clarify that the step/means d) is operative when the file is signaled as being of unknown status. By way of example without limitation, support for this feature can be found at page 3, lines 33 and 34 of the subject patent application.

The subject matter of the pending claims is fundamentally different from the system described in Roberts. By way of background, the non-limiting example embodiments described in the subject patent application relate to scanning files transferred through a network for malware and, in particular, to improving the detection of malware. See, e.g., page 1, lines 14-22 of the subject patent application. The non-limiting example embodiments can also reduce the load on the scanning system. See, e.g., page 1, lines 22-25 of the subject patent application. In the general case of scanning files transferred through a network, the amount of traffic is typically enormous and the burden of scanning is very significant indeed.

The example embodiments can provide improved scanning and reduce the scanning load based on a recognition that a significant proportion of network traffic consists of executable files which are uninfected copies of common applications and utilities. See, e.g., page 2, lines 13-16 of the subject patent application. Claims 1 and 7 implement a technique that allows files to be reliably recognized as such.

In particular, this involves a file recongiser (claim 1) or corresponding method step (claim 7) which determines "whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances." This allows the file itself to be recognised. If recognised, a difference checker (claim 1) or corresponding method step (claim 7) checks "whether the file is an unchanged version of that known program."

As a result, a file which is recognised can be signaled to be not malware if it is an unchanged version or signaled to be malware if it is a changed version. This allows positive detection of new malware in an executable program even before there has been sufficient time to develop signature-based malware detection. This is significant in the context of, for example, the rapidly changing environment of the internet.

Furthermore, a definitive positive or negative result of whether the file being transferred is or is not malware can be provided based on the simple recognising and difference checking steps without the need for a full malware scan which would require a significantly higher processing load. In this way, the load on the scanning system is reduced. This reduction is significant is the context of scanning files transferred through a network which has a high volume of traffic.

In contrast to this case of scanning files transferred through a network, Roberts is concerned with a specific case of scanning web pages passed through a firewall to implement internet browsing. Paragraph [0033] of Roberts discloses that internet addresses are identified within objects such as e-mails or files passing through the firewall. The system preemptively scans the web pages located at the identified address for malware. Paragraph [0032] discloses that the malware scanning uses "conventional techniques" and no detailed explanation is provided.

As described in paragraph [0034] of Roberts, in the event that no malware is found in the web page, the system stores the internet address in a database, together with data identifying the version of the web page including a checksum. Thus, the database stores records of internet addresses in respect of which the web page at the address has been found to be not malware in the preemptive scan.

Paragraph [0036] discloses the processing performed when a user subsequently makes an access request for the web page at an internet address. In particular, the system checks whether the internet address is stored in the database. If not, then the web page at the address is scanned for malware. But if the internet address is stored in the database, paragraphs [0037] and [0038] describe that the system checks whether the web page at

the address has changed since the preemptive scan. One described technique for doing this is to compare the checksum in the database with the new checksum for the retrieved page. If the web page has not changed, then the system supplies the web page to the user.

The purpose of the system of Roberts described for example in paragraph [0010] is to reduce the delay experienced by the user after making an access request for the web page at an internet address, e.g., by clicking on the internet address. The delay is reduced because the preemptive scan avoids the need to scan the web page again at the time the access request is made, provided the web page is unchanged. Thus, the purpose of Roberts is to speed up internet browsing.

The Section 102 rejection of the claims is based on, among other things, an allegation that the processing means/step b) of claims 1 and 7 is disclosed in paragraphs [0036] and [0037] of Roberts. However, as is clear from the above discussion, the processing means/step b) of independent claims 1 and 7 is not shown in the referenced portions of Roberts or elsewhere therein.

Roberts stores a database of internet addresses which have been preemptively scanned and found to be safe and determines whether the web page is safe to supply to the user by (i) determining whether the internet address specified in the access request by the user is present in the database (see paragraph [0036] of Roberts), and (ii) checking whether the web page at the address has changed since the preemptive scan (see paragraphs [0037] and [0038] of Roberts).

The recognition required by the claims 1 and 7 is different than anything in Roberts and involves determining "whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances." This is different than Roberts which in paragraph [0034] considers only the internet address, that is the location of the web page and does not consider the contents of the web page.

Consequently, claims 1 and 7 also contain the novel feature in means/step a) that the database contains "records of known executable programs" which includes "at least

one characteristic signature associated with each said instance [of a known executable program in the database]." This is not shown in Roberts who only stores in the database a list of internet addresses, i.e., locations in the internet. An internet address is not an executable program. Of course, there was a web page at the time of preemptive scanning, but (i) the database cannot be considered as a record of the web page because the address merely identifies the location and the web page at the location could change (which is why Roberts uses the difference check described in paragraph [0037]) and (ii) in any event a web page is not an executable program.

These differences from Roberts are significant because the system and method of the pending claims can improve the detection of malware and reduce the load on the scanning system. Such advantages cannot be obtained by Roberts.

First, Roberts uses "conventional techniques" for malware scanning, so there is no improvement in detection, just an increase in browsing speed. In particular, Roberts does not allow the detection of new malware in executable programs before there has been time to develop a signature-based scan. When Roberts detects that a web page has changed, this is not indicative of malware as web pages are frequently updated. In recognition of this, in this situation, Roberts merely subjects the web page to a new scan as described in paragraph [0038].

Second, Roberts only considers the internet address, that is, the location of a file to be transferred. Indeed, in the context of browsing, the system of Roberts actually increases the scanning load by preemptively retrieving and scanning web pages which have not been requested by the user and might not ever be requested by the user.

For at least these reasons, Applicant respectfully submits that Roberts cannot anticipate claims 1 and 7, or the claims that depend therefrom.

With respect to claims 6 and 12, Wu et al. is applied as allegedly showing the claimed exception list handler. However, Wu et al. does not remedy the deficiencies of Roberts with respect to claims 1 and 7 (from which claims 6 and 12 depend,

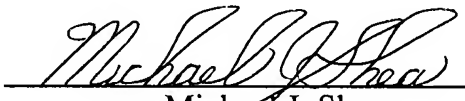
respectively). Consequently, even assuming proper motivation were to be identified for combining Roberts and Wu et al., the subject matter of claims 6 and 12 would not result.

New claims 13-16 have been added. These claims are believed to be allowable for reasons similar to those discussed above with respect to claims 1 and 7.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Michael J. Shea
Reg. No. 34,725

MJS:mjs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

Appl. No. 10/500,954
Atty. Dkt.: 117-512
ANNOTATED SHEET
SHOWING CHANGES

10/500954

small dots are deleted

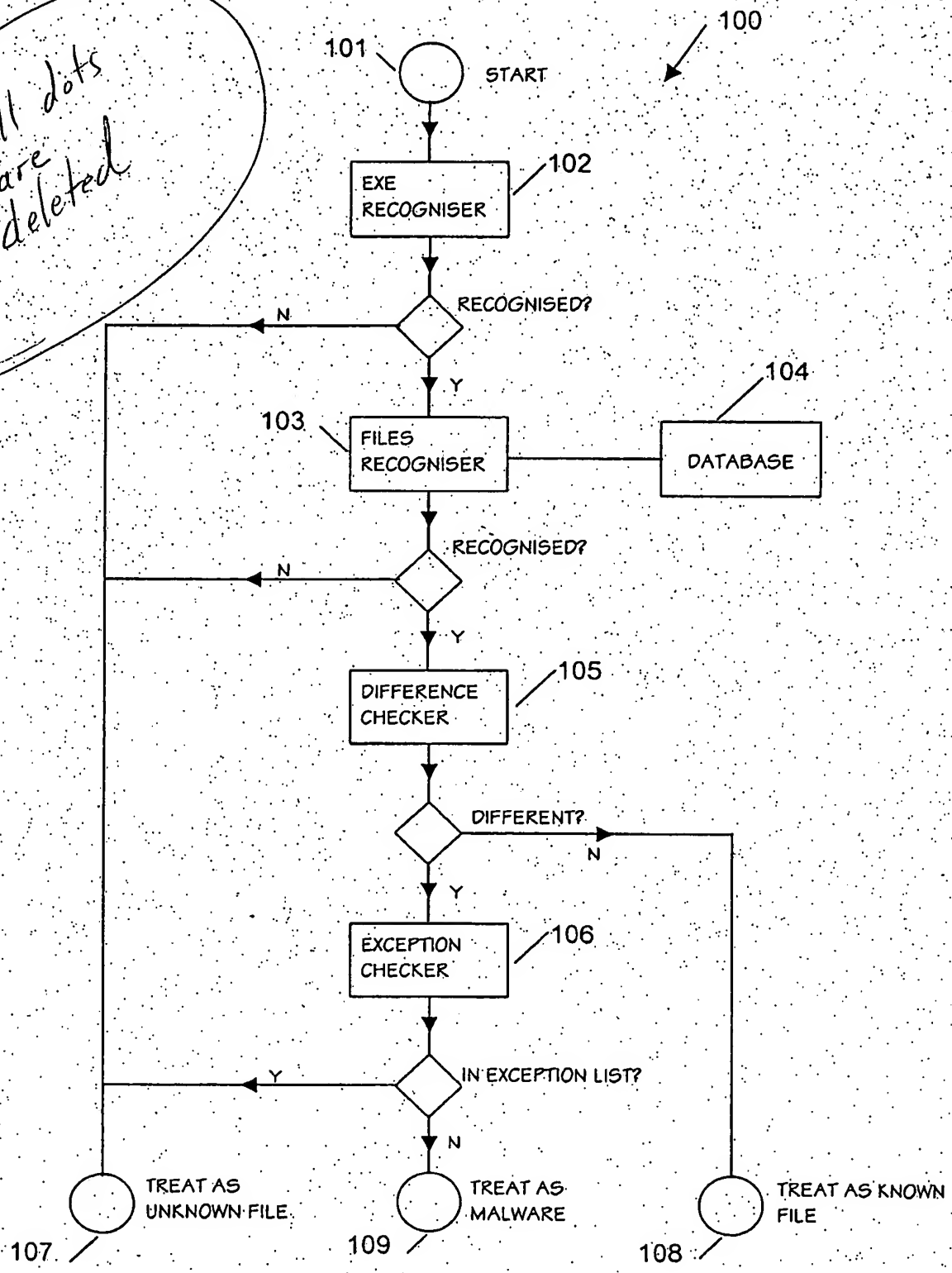


Fig.1